@chadmcrowell.com
/in/chadmcrowell
kubeskills.com

CYBR

Storage Security

@chadmcrowell.com
/in/chadmcrowell
kubeskills.com

CYBR

Defender for Storage

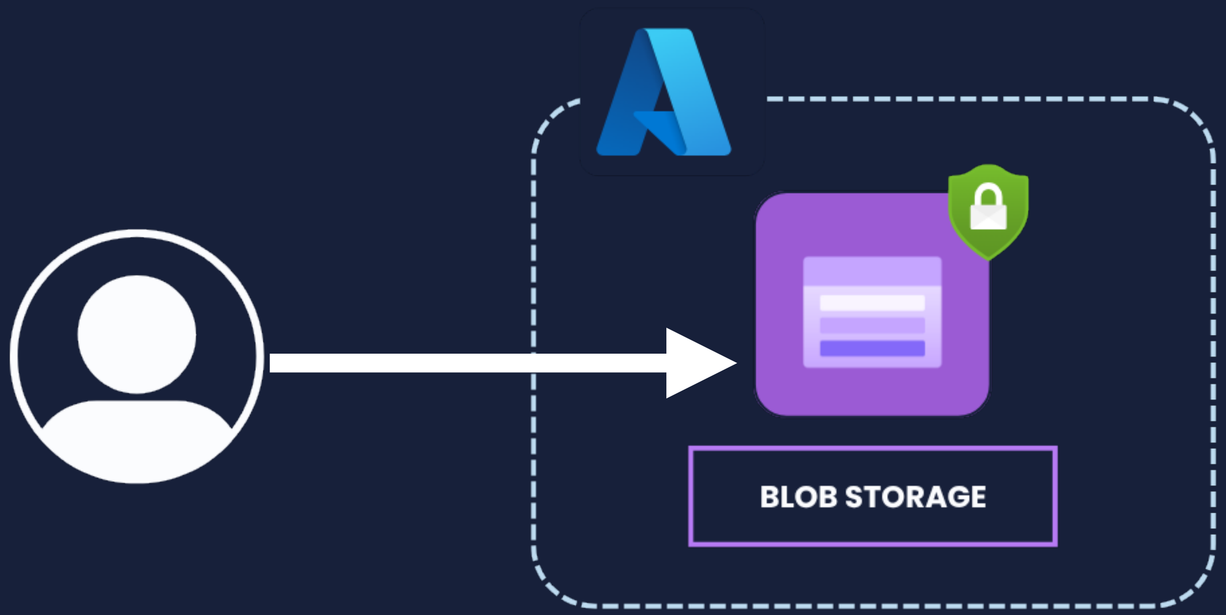
- Detects anomalous access patterns
- Identifies suspicious operations (e.g. mass file deletions or access from unfamiliar IPs)
- Integrated threat intelligence

Microsoft Defender for Cloud

@chadmcrowell.com
/in/chadmcrowell
kubeskills.com

CYBR

Defender for Containers

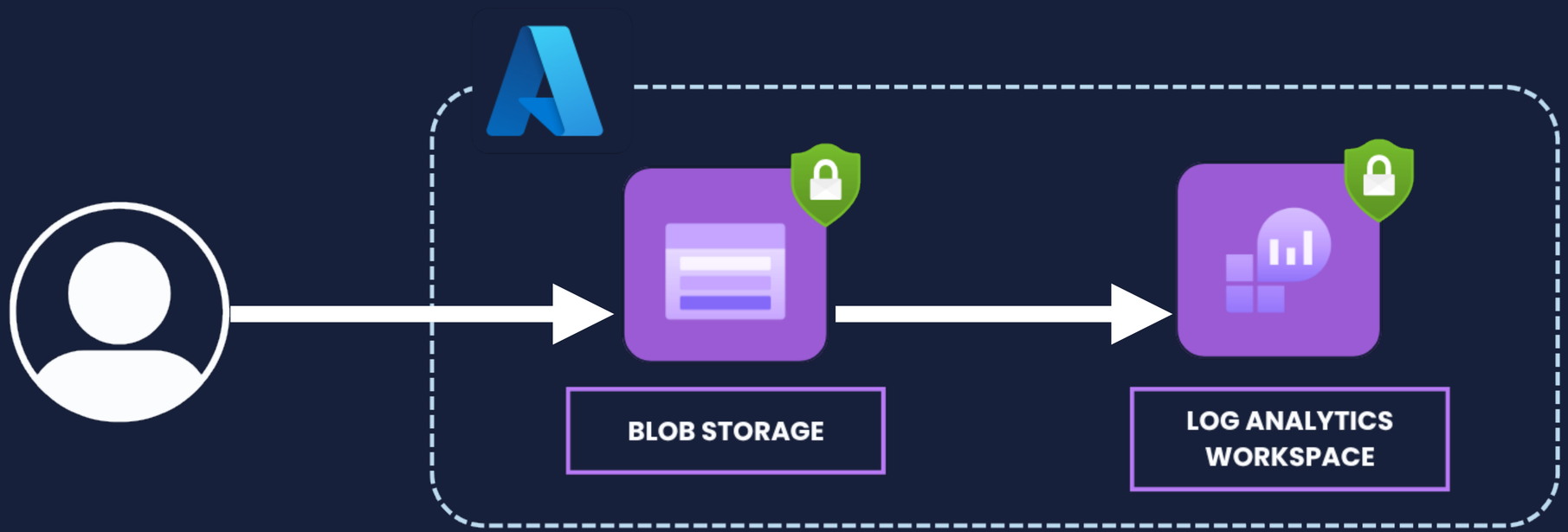


Microsoft Defender for Cloud

@chadmcrowell.com
/in/chadmcrowell
kubeskills.com

CYBR

Defender for Containers



@chadmcrowell.com
/in/chadmcrowell
kubeskills.com

CYBR

Azure Monitor Diagnostic Settings

- Storage analytics logs are deprecated
- Sends logs to Log analytics workspace (or Event Hub)
- Integrated with KQL, Microsoft Sentinel, Logic Apps, alerts, and dashboards

Microsoft Defender for Cloud

@chadmcrowell.com
/in/chadmcrowell
kubeskills.com

CYBR

Agent Protection

- Runtime Protection
- Workload behavior analysis
- Container-level anomaly detection
- Audit log monitoring

https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-enable

@chadmcrowell.com
/in/chadmcrowell
kubeskills.com

CYBR

THANK YOU!